Примена машинског учења у статичкој верификацији софтвера

Семинарски рад у оквиру курса
Методологија стручног и научног рада
Математички факултет

Лазар Ранковић, Немања Мићовић, Урош Стегић
lazar.rankovic@outlook.com, nmicovic@outlook.com, mi10287@alas.matf.bg.ac.rs

Абстракт

Верификација софтвера постаје све битнија дисциплина (реф). Класични приступи су добри, имају супер резултате (реф). Машинско учење постаје све популарније. Показаћемо преглед радова који примењују алгоритме машинског учења у циљу убрзања процеса верификације (реф).

Садржај

1 Uvod

Увод ћемо пред крај писати.

2 Верификација софтвера

Верификација софтвера је дисциплина развоја софтвера чији је циљ да се бави проверавањем да ли програм задовољава све унапред задате захтеве. Унапред задати захтев су спецификација свих жељених особина програма које се постављају пре процеса верификације. Највећа примена верификације софтвера је у оптимизацији кода и провере исправности.
Што се тиче исправности морамо направити разлику између тоталне исправности и делимичне исправности. Испитивање тоталне исправност захтева да се за све могуће улазе покаже заустављање програма, то на жалост није могуће, *"Halting problem"* је теорема која је доказана да је неодлучива. Поред тога постоји још једна теорема *"Rices theorem"* која гласи "Ни једно не тривијално семантичко својство програма није одлучиво". Према томе, због ових теорема у рачунарству је довољно показати да ће резултат евалуације програма бити валидна вредност, тачније неће се десити да програм врати вредност која није валидна.
Два приступа при верификацији софтвер су: *динамичка верификација* и *статичка верификација* којом ћемо се посебно бавити у наставку.

Динамичка верификација Динамичка верификација софтвера се врши у току извршавања програма и то најчешће скупом унапред припремљених тестова који морају бити задовољени. Очигледно је да због неисцрпне варијације могућих улаза овај вид тестирања нема за циљ валидацију програма, већ је циљ динамичке верификације проналажење грешка на неком не тривијалном скупу тестова.

Статичка верификација Статичка верификација софтвера подразумева анализу софтвера без његовог извршавања, тачније анализу кода применом неке од технника које ће бити описане у наставку. Анализа кода може бити ручна или аутоматизована. Ручна метода подразумева да човек проверава код, а аутоматизована подразумева описивање па чак и превођење кода на неки од математичких језика, изабране математичке теорије. Најчешћа употреба статичке верификације је оптимизација кода при превођењу.

3 Технике статичке верификације

Апстрактна интерпретација је је теорија семантичке апроксимације чија је идеја да направити нову семантику над програмским језиком тако да се конкретан програм увек завршава. Тако се анализа програма врши над апстрактном семантиком да би добили апроксимацију над целом семантиком. Коришћење апстрактне интерпретације се омогућава помоћу две функције: функције која пресликава конкретне вредности у апстрактне вредности и функције која слика апстрактне вредности у конкретне вредности. Неизбежно је заобићи

губљење података при пресликавању из конкретних вредности у апстрактне вредности јер је циљ показати да се над апострактном семантиком програм завршава. Користећи овај математички оквир је релативно лако показати да ако се програм завршава у новој семантици програм ће бити коректан и у стварној семантици.

Симболичка анализа је метод статичке анализе који анализира програмске вредности који могу да се мењају. Овај метод има за циљ да изведе математички модел који прецизно описује израчунавање, заправо може се посматрати као нека врста компајлера који преводи програм у симболичке изразе. Квалитет алгебарских система као што су (Axiom, Derive, Macsyma, Maple, Mathematica, MuPAD, and Reduce) је веома битан јер квалитет овог начина анализе у великој меримо зависи од паметних алгебарских упрошћавања.

Проверавање ограничених модела (енг. Bounded model checking) Проверавање ограничених модела је техника верификације која се највише користи у индустрији полуповодника, тачније верификација логичкх кола. Укратко речено смисао је да се логичка кола опишу исказном логиком. Следећи корак је провера задовољивости добијене исказне формуле. Испитивање задовољивости формула је НМ-тежак проблем, и за решавање овог питања користе се сат решавачи. Ефикасност сат решавача је од кључног значаја за ову технику. Ова техника је такође примењива и за анализу софтвера, један од начина примене је посматрање извршавања целокупног програма као скупа стања, односно као један коначни аутомат у ком се прелази из стања у стање. Ако се тако посматра програм могуће је описати сва стања искасном логиком затим повезати сва стања и тако добијену формулу пустити у сат решавач. Резултат сат решавача је може бити формула је задовољива сто би значило да је програм коректан или ако је формула незадовољива резултат ће бити контрапример којим се показује да програм није коректан и може представљати основу за дебаговање.

Литература: A Survey of Static Program Analysis Techniques [12]
A Survey of Automated Techniques for Formal Software Verification [4]

4 Машинско учење

У претходним поглављима смо представили увод у статичку верификацију софтвера. Показана је важност те области и изложене су технике верификације. Овим поглављем ћемо представити област машинског учења. Описаћемо главне аспекте ове дисциплине, показаћемо њену битност и даћемо преглед важних концепата о којима ће бити више речи у поглављу 6.

4.1 Основе машинског учења

Дефиниција 1. *"За програм кажемо да учи из искуства E кроз обављање задатка T са мером квалитета P, ако повећањем искуства E расте мера P за обављен задатак T."*

— Tom M. Mitchell *[7]*

Машинско учење можемо посматрати као област рачунарства која се бави анализом алгоритама који генерализују. Са практичног аспекта, генерализација може значити уопштавање закона над датим подацима.

Машинско учење се дели на три подобласти: *надгледано учење*, *ненадгледано учење* и *учење условљавањем*. Подаци из којих алгоритми машинског учења уче, могу бити обележени, необележени и могу се генерисати у фази учења. Оваква природа података је основ за разликовање три наведене подобласти.[7].

Међу многим проблемима над којима су често примењивани алгоритми машинског учења, издвојићемо проблем регресије и проблем класификације. Ови проблеми су релевантни за теме којих ћемо се дотаћи у овом раду. Под проблемом класификације подразумевамо испитивање инстанце датог објекта и одређивање класе којој он припада на основу његових својстава (атрибута). Типичан пример класификације је одређивање порекла тумора (испитивање да ли је тумор малигни или бенигни) на основу његове величине. Проблем регресије представља предикцију неког параметра популације за дати објекат на основу осталих атрибута тог објекта. Као пример можемо узети предикцију цене стамбеног објекта на основу његове величине, броја соба и разних других релевантних карактеристика.

Пре примене машинског учења потребно је проучити проблем који се решава, уочити његове специфичности и припремити и анализирати податке из којих ће алгоритми учити. Након детаљне анализе, врши се одабир одговарајућег математичког модела који ће нам дати одговор на проблем који решавамо. Када смо изабрали модел, вршимо његово тренирање на инстанцама припремљених података. Тренинг радимо тако што довољан број пута пуштамо модел да решава наш проблем и меримо успешност тј. грешку коју тај модел прави. Након сваког мерења, у зависности од алгоритма који примењујемо, вршимо корекцију модела у циљу минимизације грешке.

Општи опис који смо сада представили ће у даљем тексту бити детаљније образложен. Приказаћемо конкретне алгоритме и дискутовати о њиховим својствима. Алгоритме које ћемо посматрати су од велике важности за примену у статичкој верификацији, па је с тога важно њихово потпуно разумевање. Пре него што дамо преглед тих алгоритама, покушаћемо да приближимо значај машинског учења уопштено као и његов значај у статичкој верификацији.

4.2 Значајност машинског учења

Конвенционалан начин решавања проблема у рачунарству се своди на формално дефинисање низа корака који улазне параметре трансформишу не би ли дошли до резултата. Овакав приступ је користан у ситуацијама када је потребно решити проблеме који су човеку изазовни, као што су компликоване рачунске операције, сортирање великих низова и томе слично. Поставља се питање: како написати програм који би обављао задатке које човек свакодневно лако обавља? На пример, да ли је могуће написати програм који би био у стању да препознаје објекте са фотографија?

Рачунарски вид (енг. computer vision) је дисциплина која се бави овим проблемом.[3]. Алгоритми који су примењивани пре раста популарности машинског учења нису показали значајне резултате. Могли су да генеришу једноставне геометријске моделе који нису давали

задовољавајуће резултате. Дубоке неуронске мреже су алгоритами машинског учења који су показали значајне напретке у овој области [1].

Класификација дела програма на валидна стања и она која могу резултовати грешком је од кључног значаја за ефикасност алата за верификацију [2] [5]. Конкретним проблемима и њиховим решењима ћемо се бавити у наредним поглављима.

4.3 Технике машинског учења

Оптшу слику о томе како се примењују алгоритми машинског учења смо дали у уводном делу овог поглавља. Сада ћемо видети неке конкретне алгоритме и њихове особине. Како је проблем класификације централни проблем над којиме се примењује машинско учење у статичкој верификацији, описаћемо два алгоритма који решавају тај проблем. Зарад потпуности, описаћемо и један алгоритам решавања регресионих проблема.

Линеарна регресија

Као што је речено у уводном делу, регресиони проблем представља предвиђање циљне променљиве непознате инстанце на основу осталих њених атрибута. Означимо са y_i циљну променљиву, а са $\vec{x} = (x_1, x_2, ..., x_n)$ вектор атрибута које посматрамо. У примеру предикције вредности куће то могу бити број соба, квадратура куће итд. Инстанцу из скупа података онда представљамо уређеним паром $(\vec{x}_i, y_i)$. Модел линеарне регресије, параметризован вектором w, који описује законитост је следећи:

$$h(\vec{x}_i) = w^T \cdot \vec{x}_i \tag{1}$$

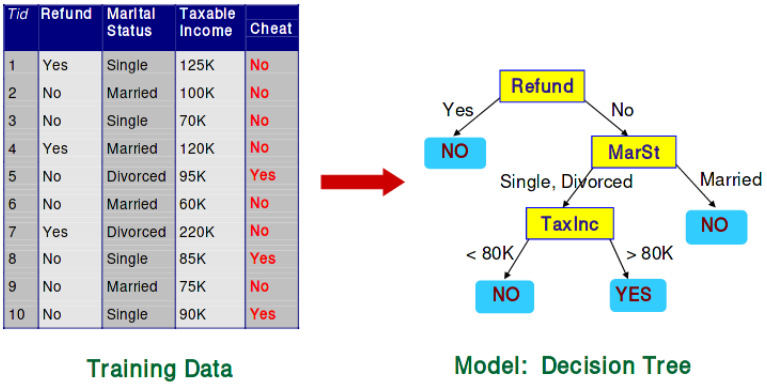
Грешка коју модел прави можемо представити погодним избором функције грешке $L(w)$. Чест избор ове функције је средњеквадратна грешка коју модел прави над свим инстанцама из тренинг скупа.

$$L(w) = \frac{1}{N} \sum_{i=1}^{N} (h(\vec{x}_i) - y_i)^2 \tag{2}$$

Тренинг вршимо тако што одређеном оптимизационом техником вршимо минимизацију функције грешке по параметрима w.

Стабла одлучивања

Стабла одлучивања представљају један од основних метода класификације. Употребу стабала одлучивања оправдава њихова висока интерпретабилност [9]. У листовима стабла одлучивања се налазе вредности циљне променљиве, односно у случају класификације, класе којима инстанца може припасти. Чворови стабла представљају атрибуте по којима се врши подела. Када су ти атрибути категоричког типа, потомци датог чвора су добијени из свих могућих вредности које тај категорички атрибут може имати. У случају да је атрибут некатегоричког типа, најчешће се врши подела могућих вредности на дисјунктне интервале тако да свако дете тог чвора одговара једном од интервала. Слика 1 приказује једно могуће стабло одлучивања добијено на основу података.



Слика 1: Стабло одлучивања

Метода потпорних вектора

Проблем класификације можемо посматрати на следећи начин. Инстанце које класификујемо представљамо тачкама у неком високодимензионалном простору. Бинарни класификатор који тренирамо је хиперраван која дели простор на два дела, тако да се у једном делу простора нађу све инстанце које припадају једној класи, а у другом делу ће се наћи оне које припадају другој класи. Раздвајајућих хиперравни може бити више, па је зато потребно одабрати хиперраван која боље описује поделу међу подацима [8].

Маргина класификације је најмање растојање између тачака које се налазе у различитим потпросторима. Слика 2 приказује хиперравни B_1 и B_2. Интуитивно видимо да ће прва хиперраван боље раздвојити податке. Маргина $(b_1 1, b_1 2)$ је значајно већа од маргине (b_{21}, b_{22}) и то је оно што први класификатор чини знатно бољим.

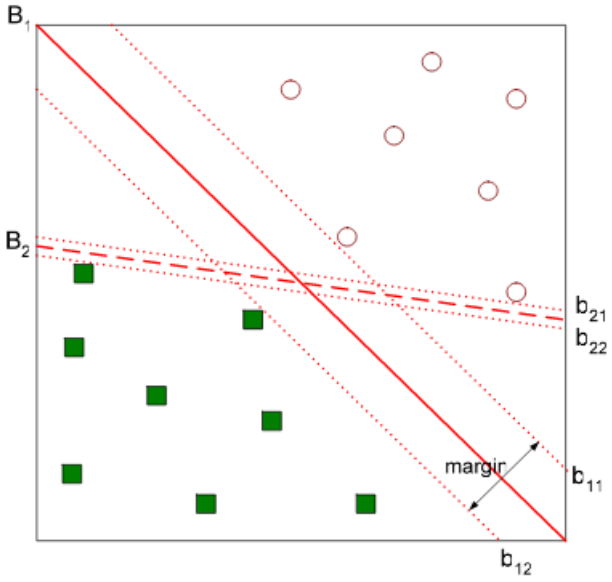
Максимизацијом маргине добијамо класификатор који боље описује поделу. Зарад конвенције, проблем максимизације сводимо на проблем минимизације, те добијамо следећи оптимизациони проблем:

$$\min_{w,w_0} \frac{\|w\|^2}{2} \tag{3}$$

Пошто смо видели основне алгоритме машинског учења, у следећем поглављу ћемо описати везу између статичке верификације и машинског учења. Бавићемо се проблемима статичке верификације који су погодни за решавање техникама машинског учења.

5 Одабрани проблеми статичке верификације

До сада смо видели стандардне проблеме и технике статичке верификације и машинског учења. У овом поглављу ћемо издвојити значајне проблеме верификације на које су, применама алгоритама машинског учења постигнути значајнији резултати.



Слика 2: Приказ различитих хиперравни

Статичка верификација мора бити у стању да разликује позитивна стања програма од негативних. Негативна су она која доводе програм до грешке. *Интерполантама* (енг. interpolants) називамо предикате који раздвајају позитивна од негативних стања. У статичкој верификацији се коришћењем оваквих интерполанти гради даљи доказ. Показано је да се ове интерполанте могу интерпретирати као бинарни класификатори. Проблем који се овде јавља је генерисање интерполанти, тј проналажење одговарајућег класификатора [10]. У делу 6.1 детаљније је описан приступ коришћен у [10].

Поред итерполанти, могуће је препознати нетривијална својства програма која даље резултују грешком. Грађењем *класификатора нетачне инваријанте* (енг. False Invariant Classifier) је могуће рангирати својства програма по томе колику вероватноћу за грешком та својства проузрокују. Одређивање нетривијалног својства датог програма је у општем случају неодлучив проблем [11, 2].

Код апстрактне интерпретације је остварив баланс између прецизности изгенерисане инваријанте и скалабилности система за верификацију. Овај баланс је последица детаљне анализе апстрактног синтаксног стабла. Одабир инваријанте је тежак проблем и показано је да се може утврдити тестирањем [10, 5].

Проблеми које смо представили овим поглављем су решена користећи одговарајуће технике машинског учења. У наредом поглављу ћемо се бавити тим решењима, даћемо увид у начине на који су та решења примењена и покушати да одговоримо на питање како наставити усавршавање тих техника.

6 Неке примене техника машинског учења у статичкој верификацији

Ово је есенција. Одабирају се проблеми из претходног поглавља и показује се како се решава. Прво иде неки уводни део, онда из литературе се покупе те технике и таксативно се наводе (принцип проблем-решење).

6.1 Проналажење интерполанти

Неформално говорећи, интерполанта представља предикат који раздваја позитивна стања програма од негативних. Примена машинског учења у проналажењу интерполанти огледа се у добијању модела који представља саму интерполанту. У делу 6.1.1 изложене су основе из [10] базиране на методу потпорних вектора, док је у делу 6.1.2 изложен приступ из рада [5] базиран на стаблима одлучивања. Експериментални резултати показали су да приступи базирани на машинском учењу јесу упоредиви са традиционалним техникама.

6.1.1 Проналажење интерполанти користећи метод потпорних вектора

Нека су A и B формуле у теорији линеарне аритметике [6].

$$\phi ::= w^T x + d \geq 0 \mid true \mid false \mid \phi \wedge \phi \mid \phi \vee \phi \mid \neg\phi \tag{4}$$

При чему је $\vec{w} = (w_1, ..., w_n)^T \in R^n$ вектор константи у простору R^n; $\vec{x} = (x_1, ..., x_n)^T$ вектор променљивих из простора R^n.

Дефиниција 2. *Интерполанта за пар формула (A, B) тако да* $A \wedge B \equiv \bot$ *је формула* I *која задовољава* $A \Rightarrow I, I \wedge B \equiv \bot$ *при чему формула* I *садржи само променљиве које се јављају у формулама* A *и* B.

На слици 3 приказан је програмски код који ће бити коришћен као илустрација. Функција непознат број пута инкрементира променљиве x и y, потом их декрементира све док променљива x не постане 0. Коначно, уколико је $y \neq 0$ онда програм одлази у стање грешке. Приметимо да је инваријанта $x = y$ довољна да се докаже да програм никад неће доћи у стање грешке.

```
foo( )
{
1:  x = y = 0;
2:  while (*)
3:   { x++; y++; }
4:  while ( x != 0 )
5:   { x--; y--; }
6:  if ( y != 0 )
7:    error() ;
}
```

Слика 3: Пример кода

Претпоставимо да је функција `foo()` извршила на следећи начин (у заградама су хронолошки наведени линије инструкција): $(1, 2, 3, 2, 4, 5, 4, 6, 7)$

који води у стање грешке. Поделимо ток на два скупа, A и B и пронађимо интерполанте за наведени ток.

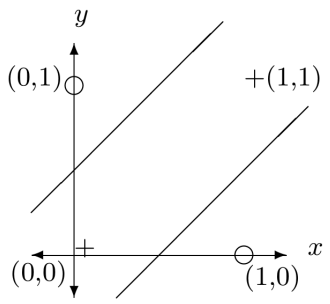
Скуп A садржи вредности x и y које се добијају након извршавања линија 1, 2 и 3. У скупу B се налазе оне вредности x и y које би се добиле уколико би програм извршио линије 4, 5, 6 и 7 чиме би програм дошао у завршно стање.

Имамо да $A \wedge B \equiv \bot$ при чему важи:

$$A \equiv x_1 = 0 \wedge y_1 = 0 \wedge if\_then\_else(b,\ x = x_1 \wedge y = y_1,\ x = x_1 + 1 \wedge y = y_1 + 1)$$
$$B \equiv if\_then\_else(x = 0,\ x_2 = x \wedge y_2 = y,\ x_2 = x - 1 \wedge y_2 = y - 1) \wedge x_2 = 0 \wedge \neg(y_2 = 0)$$

A представља скуп достижних стања док B представља скуп стања која воде у стање грешке. Интерполанта је доказ да су скупови A и B дисјунктни и изражава се користећи заједничке променљиве из скупова A и B. Затим, помоћу доказивача теорема се рачунају вредности за (x, y) које задовољавају формуле A и B [10].

Добијене вредности представљају скуп инстанци над којим се може тренирати класификациони модел (попут логистичке регресије или потпорних вектора). Позитивне инстанце представљају вредности променљивих које задовољавају формулу A и аналогно, негативне инстанце представљају вредности променљивих које задовољавају формулу B.



Слика 4: Класификација у тражењу интерполанти

Слика 4 приказује вредности променљивих (x, y) за A као плусеве (тачке $(0, 0)$ и $(1, 1)$) и B као кружиће (тачке $(1, 0)$ и $(0, 1)$). Приказани модел је добијен коришћењем метода потпорних вектора. Резултујуће праве одговарају једначинама:

$$e_1 : 2y = 2x + 1$$
$$e_2 : 2y = 2x - 1$$

Интерполанта која се одавде може извести је

$$2y \leq 2x + 1 \ \wedge 2y \geq 2x - 1$$

Овај предикат представља инваријанту чијим доказивањем се показује да програм не може доћи у стање грешке. Једноставнија интерполанта $x = y$ се може добити транслирањем добијених правих што ближе позитивним истанцама, докле год се одржава сепарабилност позитивних и негативних инстанци.

Табела 1 приказује резултате из [10] на неким од познатих примера. Интерполанте које су означене са *исто* су интерполанте које су добијене користећи решавач OpenSMT.

Табела 1: Добијене интерполанте на неким од познатијих тест примера у области.

Датотека	Време (с)	Интерполанта
f1a	0.022	((y = 1 | x <= 0) & x = 1) | (y = 0 & (y = 1 | x <= 0))
ex1	0.021	xa + 2*ya >= 0 | xa + 2*ya >= 5 | xa + 2*ya >= 5
f2	0.20	y <= 3*x | y <= 3*x + 1 | y <= 3*x + 1
nec1	није доступно	Није пронађена
nec2	0.018	x < y (исто)
nec3	0.016	y <= 9 (исто)
nec4	0.021	(x = y | y = 0) | (y = x) | (y = x)
nec5	0.018	s >= 0 (исто)
pldi08	0.017	y > x
fse06	0.017	y + x >= 0 & y >= 0 & y >= 0 & y >= 0

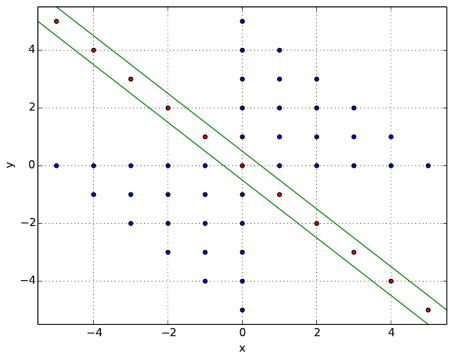
6.1.2 Проналажење интерполанти користећи стабла одлучивања

Интерполанте се могу извести и другим методима машинског учења. Рад [5] илуструје приступ који користи стабла одлучивања. За програмски код се генеришу позитивне и негативне инстанце над којима се гради стабло одлучивања користећи похлепни алгоритам. Правила добијена у стаблу се трансформишу у формулу која се потом проверава да ли је инваријанта користећи SMT решавач.

Резултати су показали да једноставни похлепни алгоритам који гради стабло даје и једноставне формуле за интерполанте. Стабло је лако научило комплексне бинарне инваријанте као једноставне коњункције.

Слика 5 приказује пример програма и његова стања која се могу добити на основу покретања самог програма. Добра стања можемо добити пратећи претпоставке (линија 2), бележећи ток променљивих и провером да ли је испуњен услов $x \neq 0$ са линије 12. Лоша стања можемо добити игноришући услов са линије 2. На пример, тачка $(-2, -2)$ тачка $(-4, -4)$ представљају лоша стања.

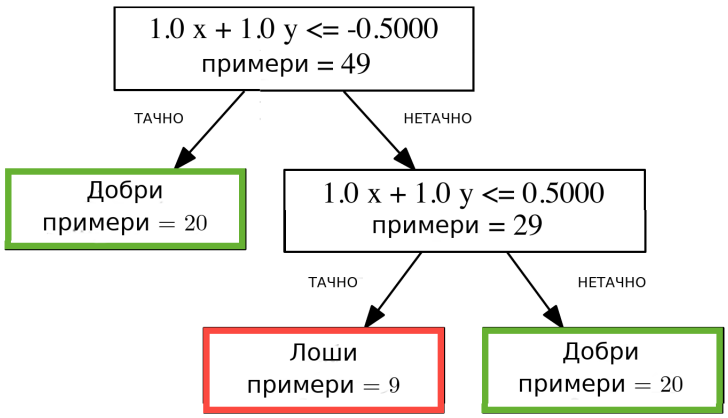
```
1  var x, y: Int;
2  assume x = 0 ∧ y ≠ 0;
3
4  while (y ≠ 0) {
5    if (y < 0) {
6      x := x − 1; y := y + 1;
7    } else {
8      x := x + 1; y := y − 1;
9    }
10 }
11
12 assert x ≠ 0;
```



Слика 5: Пример програма. Лева страна приказује код, десна страна садржи добра стања (плаве тачке) и лоша стања (црвене тачке).

Слика 6 приказује стабло добијено применом алгоритма описаног

у [5]. Добијени алгоритам је сложености $O(mn\log(n))$, где је m број атрибута а n број инстанци.



Слика 6: Стабло одлучивања добијено за пример са слике 5.

6.2 Грађење класификатора нетачне инваријанте

7 Закључак

Овде машти на вољу.. :)

Литература

[1] Deep image: Scaling up image recognition. *CoRR*, abs/1501.02876, 2015. Withdrawn.

[2] Yuriy Brun. Finding latent code errors via machine learning over program executions, 2004.

[3] Christopher M. Brown Dana H. Ballard. *Computer vision*. Prenice-Hall, Inc., 1982.

[4] Vijay D'Silva, Daniel Kroening, and Georg Weissenbacher. A survey of automated techniques for formal software verification. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD)*, 27(7):1165–1178, July 2008.

[5] Siddharth Krishna, Christian Puhrsch, and Thomas Wies. Learning invariants using decision trees. *CoRR*, abs/1501.04725, 2015.

[6] Daniel Kroening and Ofer Strichman. *Linear Arithmetic*, pages 111–147. Springer Berlin Heidelberg, Berlin, Heidelberg, 2008.

[7] Tom M. Mitchell. *Machine Learning*, volume 1. McGraw Hill, 1997.

[8] John Shawe-Taylor Nello Christianini. *An introduction to support vector machines*, volume 1. Cambridge university press, 2000.

[9] David Landgrebe S. Rasoul Safavian. A survey of decision tree classifier methodology, 1991.

[10] Rahul Sharma, Aditya V. Nori, and Alex Aiken. Interpolants as classifiers.

[11] Alan M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 2(42):230–265, 1936.

[12] Wolfgang Wögerer and Technische Universität Wien. A survey of static program analysis techniques, 2005.